JC04 Rec'd PCT/PTO 0 9 APR 2001

FORM PTO-1390 (REV. 11-2000) U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER: 704-X00-047US

U.S. APPLICATION NO. (If known, see 37 CFR 1.5): 09/807099

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/US00/21615	AUGUST 8, 2000	

TITLE OF INVENTION: HONESTY PRESERVING NEGOTIATION AND COMPUTATION

APPLICANT(S) FOR DO/EO/US: BINYAMIN PINKAS & SIMEON NAOR

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. [x] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. [ ] This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. [x] This is an express request to begin national examination procedures (35 U.S.C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. [ ] The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. [x] A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. [x] is attached hereto (required only if not communicated by the International Bureau).
   b. [ ] has been communicated by the International Bureau.
   c. [x] is not required, as the application was filed in the United States Receiving Office (RO/US).
6. [ ] An English language translation of the International Application as filed (35 U.S.C. 371(c)(2)).
   a. [ ] is attached hereto.
   b. [ ] has been previously submitted under 35 U.S.C. 154(d)(4).
7. [ ] Amendments to the claims of the International Aplication under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. [ ] are attached hereto (required only if not communicated by the International Bureau).
   b. [ ] have been communicated by the International Bureau.
   c. [ ] have not been made; however, the time limit for making such amendments has NOT expired.
   d. [ ] have not been made and will not be made.
8. [ ] An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. [x] An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
10. [ ] An English lanugage translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. [ ] An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. [x] An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. [x] A FIRST preliminary amendment.
14. [ ] A SECOND or SUBSEQUENT preliminary amendment.
15. [ ] A substitute specification.
16. [ ] A change of power of attorney and/or address letter.
17. [ ] A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821 - 1.825.
18. [ ] A second copy of the published international application under 35 U.S.C. 154(d)(4).
19. [ ] A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
20. [x] Other items or information:
    COPY OF PCT REQUEST, AMENDED PAGES, FORMAL DRAWINGS AND TRANSMITTAL LETTER; EXPRESS MAILING CERTIFICATE, POSTCARD

09807099 090401

09/807099 | INTERNATIONAL APPLICATION NO. PCT/US00/21615 | JC02 Rec'd PCT/PTO 09 APR 2001 | ATTORNEY'S DOCKET NUMBER 704-X00-047US

21. [x] The following fees are submitted:	CALCULATIONS PTO USE ONLY	
BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):		
Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**		
International preliminary examination fee (37 CFR 1.482) not paid to USPTO but international search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**		
International preliminary examination fee (37 CFR 1.482) paid to USPTO and all claims satisfied provisions of PCT Article 33(1)-(4) **$100.00**		
ENTER APPROPRIATE BASIC FEE AMOUNT =	$ 710	
Surcharge of **$130.00** for furnishing the oath or declaration later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(e)).	$	

CLAIMS	NUMBER FILED	NUMBER EXTRA	RATE		
Total claims	22 - 20 =	2	x **$18.00**	$ 36	
Independent claims	- 3 =		x **$80.00**	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+ **$270.00**	$	
TOTAL OF ABOVE CALCULATIONS =				$ 746	
[x] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2.			+	$ 373	
SUBTOTAL =				$ 373	
Processing fee of **$130.00** for furnishing the English translation later than [ ] 20 [ ] 30 months from the earliest claimed priority date (37 CFR 1.492(f)).				$	
TOTAL NATIONAL FEE =				$ 373	
Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property +				$ 40	
TOTAL FEES ENCLOSED =				$ 413	
				Amount to be refunded:	$
				charged:	$

a. [ ] A check in the amount of $ _____ to cover the above fees is enclosed.

b. [x] Please charge my Deposit Account No. 50-0601 in the amount of $ 413 to cover the above fees. A duplicate copy of this sheet is enclosed.

c. [x] The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 50-0601 A duplicate copy of this sheet is enclosed.

d. [ ] Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

MARTIN FLEIT
FLEIT KAIN GIBBONS GUTMAN & BONGINI
520 BRICKELL KEY DR. #A201
MIAMI, FL 33131

Martin Fleit
SIGNATURE

MARTIN FLEIT
NAME

16,900
REGISTRATION NUMBER

09/807099
JC02 Rec'd PCT/PTO 09 APR 2001

PATENT - Attorney Docket No.: 704-X00-047US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Appln of: BINYAMIN PINKAS ET AL

Appln. No/Patent No.: National Stage filing based on PCT/USOO/21615

Filed/Issued: April 8, 2001

For: HONESTY PRESERVING NEGOTIATION AND COMPUTATION

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D. C. 20231

Sir:

IN THE CLAIMS:

For the above-entitled matter, kindly amend the claims as follows:

- - 3. (amended) The method according to [any one of claims 1 or 2] claim 1, for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount to be paid, and wherein the center only makes disclosure to the winning bidder, while all other bidders being able to verify that the auction was computed correctly, but do not learn any other information.

- - 4. (Amended) The method according to [any one of claims 1, 2 or 3] claim 1, for first price auctions, where the output of F is (B.sub.j, X.sub.j), where X.sub.j is greater or equal to any one X.sub.i for 1 <=i <=n.

- - 5. (Amended) The method according to [any one of claims 1, 2 or 3] claim 1, for second price auctions (Vickrey auctions), where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is greater or equal to any X.sub.i for 1 <=i <=n except for i=j1.

- - 6. (Amended) The method according to [any one of claims 1, 2 or 3] claim 1, for k-th price auctions, where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is the k-th largest among all inputs X.sub.i for 1 <=i <=n.

- - 7. (Amended) The method according to [any one of the preceding claims] claim 1 wherein the auction is a plural auction where there are a plurality of sellers.

- - 8. (Amended) The method according to [any one of the preceding claims] claim 1 wherein the auction is a generalized Vickrey auction.

- - 9. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of, computing the auction such that the auctioneer wants to buy an item and each of the bidders wants to sell this item, and wherein negative values of the inputs X.sub.i are possible.

- - 10. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of; computing the output of the auction such that the users learn, in addition, some statistic of the inputs, such as, the users can learn at least one of the average of the inputs, the variance of the inputs, or how many one inputs were in a certain range.

- - 11. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of computing the output of the function such that only the center learns the output of the function. or several of the users learn the output of the function, or all the users learn the output of the function.

- - 12. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of, computing the output of a mechanism, in particular, for one of Groves-Clark mechanisms, opinion polling and stable matching.

- - 13. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the steps of each user committing to the values of his input in a manner that the user cannot change it afterwards, but hiding the input value from the center,[.]at a specific stage, the users opening their commitments to their inputs and revealing their values to the center, which then computes the value of F in a manner the each of the users can verify that the values that were used as inputs for computing F were the values that were committed to by the users.

- - 14. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of implementing automated agents which participate in the auction which do not disclose to the auctioneer the limit price that they were given, until the end of the bidding period.

- - 15. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of computing a function where the center can generate a proof that it computed the correct output of the function.

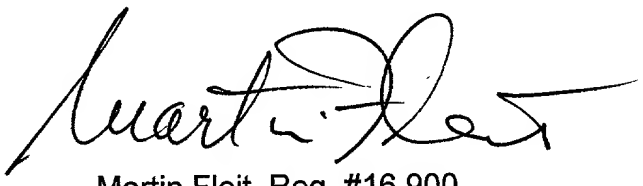
- - 16. (Amended) The method according to [any one of the preceding claims] claim 1, comprising the step of computing a function by N centers, such that only if K of the N centers collude they can learn information about the parties' inputs.

PCT/US00/21615 05/02/2002

REMARKS

The above amendments are to remove multiple dependencies.

Respectfully submitted,



Martin Fleit, Reg. #16,900

Martin Fleit
FLEIT KAIN GIBBONS GUTMAN & BONGINI
520 Brickell Key Drive #A201
Miami, Florida 33131
Tel: 305-536-9020; Fax: 305-536-9022
e-mail: MFleit@FleitKain.com

TRANSMITTED: 06/07/2002

6/PRTS

09/807099
JC02 Rec'd PCT/PTO 09 APR 2001

HONESTY PRESERVING NEGOTIATION AND COMPUTATION

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates generally to cryptography and to secure distributed computation, and more particularly it relates to computerized auctions conducted using PCs and/or servers over a network, such as, the Internet.

Description Of The Prior Art

An exciting topic of cryptographic research is secure function evaluation [see e.g. REFERENCES 3, 7, the citations for which are given in detail at the end of the specification]. For any function F(x.sub.1, x.sub.2,...,x.sub.n), it is possible, in principle, to construct a protocol that allows a group of n parties, where party i has as its private input x.sub.i, to jointly evaluate F(x.sub.1, x.sub.2,...,x.sub.n). Following the protocol the parties learn F(x.sub.1, x.sub.2,...,x.sub.n) but no party i can learn about the inputs other than x.sub.i more than can be computed from x.sub.i and F(x.sub.1, x.sub.2, ..., x.sub.n). The drawback of these protocols is that they are rather complex and require a lot of interaction between each of the parties. In the case of auctions this would require high interaction between the bidders, who have no motivation to interact with each other. The present invention, as will be described in greater detail in the following, provides a much simpler method in which all the parties communicate with just a single center. In the inventive method described hereinafter, the input of each of the parties becomes known to this center but otherwise, it is not known to any other party. The inventive method enables the center to prove that it preformed the computation correctly.

In the case of auctions, it is normally the case that the auctioneer is trusted by all parties to compute the result of the auction correctly. This might not be justified, since the auctioneer might benefit from an illegal modification of the result of the

auction. (This is even true if the auctioneer is just a mediator that is selling items which are offered by third parties, since such auctioneers usually charge a commission which depends on the price with which the items are sold). It is sometimes the case that a trusted party (say an accountant) observes the operation of the auctioneer and testifies that it is trustworthy. However this party might be corrupted and cooperate with a corrupted auctioneer, it might also be the case that the trusted party cannot watch the auctioneer closely enough and the auctioneer can cheat without being detected. These problems are amplified in a computerized Internet setting.

The center that computes F can of course prove that it computed it correctly by publishing all the inputs. However this solution affects the privacy of the other parties, since their inputs become public. The inventive method overcomes this problem since it enables the center to prove that it computed F correctly without leaking any information about the inputs.

There are suggestions in the art for distributing the operation of an auctioneer between many servers in a way which is secure as long as not too many of these servers operate maliciously. Franklin and Reiter [see REFERENCE 2] developed a distributed system for sealed-bid auctions with many auctioneer servers, which ensures the privacy of the bids until the time they are opened. This system further enables the bids to be backed by escrowing financial commitments of the bidders. Harakavy, Tygar, and Kikuchi [see REFERENCE 4] present systems for secure first price and second price sealed bid auctions, which preserve the privacy of the bids even after the winning bid is chosen (this variant was also briefly mentioned in REFERENCE 2). Both systems distribute the operation of the auctioneer between several servers and privacy is guaranteed as long as not too many of the servers collude (most of the protocols require that less than a third of the servers collude, and therefore, need a minimum of four servers). However, if enough auctioneer servers collude they are able to maliciously change the outcome of the auction and would not be detected. The requirement that auctioneer servers would not collude seems very hard to enforce since all these servers operate for the auctioneer which might have a motivation to cheat and increase its profits. Compared to these prior art solutions, the inventive method does not require to distributing the operation of

the auctioneer among several non-colluding servers, and provides security even if the auctioneer is attempting to cheat.

Naor and Pinkas [see REFERENCE 6] present a different method that prevents even the center from learning information about the parties' inputs. That method requires the operation of an additional party - the Issuer. The Issuer generates a program that computes the function (or the auction) and sends it to the center. The center receives messages from the parties, which contain some information that is intended for the Issuer. After the center receives messages from all the parties it sends a message to the Issuer and receives a response which enables it to use the program to compute the output of F for the parties' inputs. The method ensures that neither the center nor the Issuer learn information about the inputs of the parties. In this sense it provides better privacy than the inventive method described herein. However, the inventive method presented here does not require the cooperation of any additional party (like the Issuer) for the computation of F. It enables the center to compute the function by itself and prove that it computed it correctly, and in this respect is an advantage.

T06040 - 56/70860

SUMMARY OF THE INVENTION

Consider a scenario with N parties, each having a private input, and a single center. There is a function F with N inputs whose output should be computed. Each party sends its input to the center. The present invention is a method, system and apparatus that enables the center to compute and publish the output of F and to prove to all parties that it computed F correctly. This is done without revealing the value of the input of a party to any other party.

More specifically, the parties can be bidders in an auction, their inputs are their bids, the center is the auctioneer, and the program F expresses the rule by which the outcome of the auction is decided. The invention requires the auctioneer to prove that it computed the result of the auction correctly.

The invention provides the same security as in the following scenario: Assume that there is a reliable party (say an accountant or a lawyer) which is trusted

by all other parties. This party observes the operation of the center, i.e. it examines the inputs that the center receives, verifies that the center computes the correct output, and testifies that this is the case. The invention provides the same security as is provided with this trusted party, but without using any such party. This ensures better security (since trusted parties might breach the trust they are given), and is more efficient (since it does not require an additional party).

Other and further advantages and objects of the present invention will become readily apparent when considering the following detailed description of the present invention when taken together with the appended drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a block diagram illustrating the different entities engaged in a computerized auction.

Figure 2 is a schematic diagram illustrating the steps of the method of the present invention where the steps are indicated by numerals in parentheses.

Figure 3 is a high level descriptive flow chart of the present invention as generally depicted in the diagrams of Figures 1 and 2.

Figure 4 is a flow chart showing the steps of the implementation of the preferred embodiment of the present invention.

Figure 5 is a flow chart of a secure two-party function evaluation protocol as implemented by the present invention.

Figure 6 is a schematic diagram of a gate used in the protocol depicted in Figure 5, and also shows the pseudo-random function used to prepare Table T_g used in the protocol of depicted in Figure 5.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

As initially noted, the apparatus and method of the present invention comprises an auction service that is used in a network, such as, the Internet, and uses clients and/or servers. The invention utilizes cryptography and secure distributed computation via computers to effect a computerized auction. However, the invention is not limited to computerized auctions, but has broader application.

Many such applications involve a group of participants, denoted herein as "Parties", each of whom has an input to the group as a whole, where the group as a whole is required to compute and output a certain function of these inputs. The term "function" herein denotes, in the usual sense, any mathematical or logical mapping from one set of input entities to an output entity or set of entities. In certain cases, the inputs may involve sensitive information, such that it would also be required that this computation does not reveal any information about the inputs, except for whatever might be computed from the final output. Such inputs are herein denoted as "private inputs". If, in addition to the parties, there were furthermore a trustworthy participant, denoted herein as a "center" and which is trusted by all the parties, then each party could simply send the respective private input to this center, which would then compute the function and publish, or output, the value of the computed function. (The center is a participant in the protocol and is involved in the computation of the function. It may or may not have a private input, and may or may not be within the group of parties.) The parties, however, might not trust each other, and might not trust any single center.

Although a particular case of interest is that of auctions, for example, sealed-bid second-price auctions, commonly known in the art as "Vickrey auctions", other applicable activities include mechanism design, which deals with the design of protocols for selfish parties. The goal of a protocol is to aggregate the preferences of the parties in order to decide on some social choice (for example, to decide whether a community should build a bridge, or how to route packets in a network, or to decide who wins an auction). Each party has a utility function which expresses how much that party values each possible outcome of the protocol (the bid in an auction, for example, is such a utility function). Each party sends information about its utility function to a center, which decides on the outcome of the protocol based on the reports from the parties, according to a specified function of the utility functions (for example, in a sealed-bid auction, the specified function that determines the winner is the maximum of the bids). The creation of algorithms by mechanism design is known in the art, to solve a global problem among a number of selfish agents (e.g. routing, or some cooperation between the agents). The present invention can be used to compute these algorithms without requiring trust in the center. The plausibility of using the present invention for such a task depends on the

complexity of expressing the utility functions and decision procedure in terms of circuits.

A particular case of interest is the Groves-Clarke mechanism, where the public good is served if the sum of reported values is higher than some threshold. The circuit which computes this function is very simple, as is the circuit which computes the sum of the reported values for several options, and decides on the option with the highest sum. It is therefore very easy to use the present invention to provide a private protocol which computes a Groves-Clarke mechanism.

Opinion polling is another relevant application. The design of mechanisms to elicit opinions of a group of independent experts. The application enables parties to contribute their opinion to a decision making without being worried that their opinion would be revealed. It is known in the art that where experts want their recommendation to be accepted, that there exists a mechanism with a single equilibrium which achieves the public target (but such a mechanism does not exist if experts care only about the public good). Such a mechanism can be implemented very efficiently by the present invention. This essentially requires that one expert chooses a subset of the experts whose opinions are considered, learns their opinions, and then adds his opinion. The group decision is the majority opinion.

Another application is for polling the opinions of a group of people, while hiding the individual opinions of the participants. Consider for example an opinion poll (such as the Gallup Poll) which contains many questions. Suppose that the poll is anonymous, and the organizer obtains lists of answers, one list for each participant. In order to prove that it computed the result correctly, the organizer must publish the lists of answers. Suppose also that only a single participant answered affirmatively to a certain question, and that it is possible to guess with very high probability who this participant is. Then, although the answers are anonymous, it is possible to learn the answers of this participant to all the questions. The present invention enables the sending of questions to the group members, and the processing of their answers to obtain commutative outputs without revealing any information about individual answers. Additional applications of the present

invention include multiple-question opinion polls, sociometric research, and voting and elections.

Stable matching is yet another example of a global decision which depends on the private preferences of many parties. In many scenarios it is plausible that parties would be hesitant to reveal their matching preferences, even to the center that computes the matching (consider, for example, matching couples for a prom). The present invention enables the parties to reveal their true preferences without being afraid that the center can leam them. As with other applications, the overhead of implementing the present invention for this application depends on the complexity of expressing the matching algorithm as a combinatorial circuit.

Referring now to the drawing, the different entities are depicted in Figure 1. As shown, the entities include **The parties 320** and the **Center 321**. Each of the parties **320** has an input to the function F. In the case of auctions some of the parties might wish to sell items, and the rest of the parties are interested in buying these items. In addition to the parties 320, there is a **center 321.** The center **321** runs the show: it advertises the fact that F is computed, receives the inputs, and performs the computation. In the case of auctions, the center is the auctioneer. It publishes the auction, receives the bids from the bidders, and computes the outcome of the auction. The auctioneer might be a party which merely organizes the auction. It is also possible that it is one of the bidders or one of the sellers (for example he is selling an item which all other bidders are interested in buying).

The Steps in a high level description of a preferred embodiment are illustrated in Figure 2. The high level description of the illustrated preferred embodiment of the method involves the following sequence of steps of the protocol. The Steps include the following sequence. (1) The center announces the computation and commits to the circuits. (2) Party 1 sends a commitment to its input (Party 1 represents a generic party, and this operation is performed by each of the participating parties). (3) The center publishes the commitments. (4) Party 1 opens its commitment, and the center

verifies it. (5) The center computes the function. (6) The center publishes a proof that the computation was correct, and Party 1 verifies it.

The Steps of the method of the present invention are elaborated in more detail in the following, with reference to Figure 3. As shown, there are a number of bidders 320 and a single center 321. The center announces Step **301** that it will compute the function F. (In the case of an auction the auctioneer announces the existence of the auction and publishes its rules). The center publishes in Step **302** commitments to K combinatorial circuits **322** that compute F (where K is a security parameter).

Party B.sub.i, which wishes to participate in computing the function F, sends a message to the center. They might exchange several rounds of communication, Step **303,** at the end of which the center has a commitment c.sub.i to the value of B.sub.i's input x.sub.i.

The center publishes in Step **304** the commitments it received from the parties. (In the case of auctions this can be done at the end of the bidding period).

In Step **305** the bidders choose part of the K circuits that the center committed to, from block **323,** and ask the center to open them. They verify in Step **306** that the circuits compute the function F. In Step **307** each party B.sub.i sends to the center the value x.sub.i to which it committed with c.sub.i. The center verifies that x.sub.i corresponds to c.sub.i, that is it verifies that A(x.sub.i,c.sub.i)=1.

The center now computes in Step **308** the value of the circuit that computes F for the inputs x.sub.i it received. Next, the procedure for verifying the computation takes place. The center computes and publishes a proof in Step **309** that it computed the value of F correctly. Each party can use the published commitments to verify in Step **310** that the proof is correct.

A considerable improvement to the protocol can be achieved by noting that the function that is computed by the circuit need not be the function F that the center

computes, and whose computation should be verified. The circuit can compute a function F' that **verifies** that F was computed correctly. For example, if F is a function that computes the value and the index of the maximum of N inputs, X(1),...,X(N), F' is the following function: It has N+2 inputs comprised of the N inputs to F and the outputs (j,Y) of F. F' outputs 1 if and only if X(j)=Y, and X(j)>=X(i) for every i different from j. The circuit that computes this function is substantially more efficient that the circuit computing F.

There now is elaborated a detailed description of the preferred embodiment . The inventive method employs cryptographic tools that enable a secure two-party function evaluation. The particular secure two-party function evaluation protocol used in the present invention is based on the method disclosed in REFERENCE 7. In the invention, the protocol is run between two participants, ***A*** and ***B***. The input of ***A*** is a value *x* and the input of ***B*** is a description of a function ***f***. At the end of the protocol, ***A*** learns ***f***(*x*) (but no other information about ***f***), and ***B*** learns nothing about *x*. Thus, the input *x* is a private input of ***A***, and the function ***f*** is a private input of ***B***.

The protocol is based on expressing ***f*** as a combinatorial circuit of gates which are over some fixed base (e.g. all the functions **g**: 0,1 times 0,1 to 0,1). The bits of the input are entered into input wires and are propagated through the gates.

This procedure encrypts a circuit by generating a pseudo-random isomorphic transformation of the circuit. This encryption is herein referred to as a "garbling" of the circuit. The cyphertext of a circuit so encrypted by this procedure is herein denoted as a "garbled" circuit. This process is detailed below, with reference to Figure 5.

As shown in Figure 5, Inputs **502** include: ***A:*** a value *x*, in an input **502-A**, and ***B:*** a description of a combinatorial circuit which computes ***f***, in an input **502-B**. The outputs of the flowchart shown in Figure 5 are Outputs **536** that include: ***A:*** ***f***(*x*), in an output **536-A**, and ***B:*** nothing, in an output **536-B**.

The protocol starts with Initialization. In step **504, *B*** devises a circuit **506** made of logic gates, such that circuit **506** computes ***f***. The design of logic circuits made of gates that compute functions is well-known in the art.

Next, the circuit is encrypted. In step **508, *B*** assigns to each wire i of circuit **506** two random values (W_i^0, W_i^1) **510** corresponding to 0 and 1 values of wire i. The random values should be long enough to be used as keys (for example, 80 bits long). The value of wire i is denoted by b_i. In step **512, *B*** also assigns to wire i a random permutation π **514** over 0,1, π_k: $b_i \rightarrow c_i$.

In step **516, *B*** uses a pseudo-random function R **518** to prepare a table T_g **522** (or a set of tables, also denoted herein by T_g) which enables computation of the garbled output of each gate **g 520**, $(W_k^{b_k}, c_k)$, from the values $(W_i^{b_i}, c_i)$, $(W_j^{b_j}, c_j)$, the garbled inputs to gate **g**. Table T_g does not disclose any information about the output of gate **g** for inputs other than the pair (b_i, b_j), nor discloses the values of the bits b_i, b_j, or b_k.

In step **524, *B*** prepares an output translation table T_O **526** which decrypts the garbled output bits of the circuit (the cyphertext output) to the actual bits of the output of the circuit (the cleartext output).

Figure 6 illustrates gate **g 520**, which is a generic gate that computes the value b_k of an output wire k **604** as a function of the values b_i, and b_j of input wires i **606** and j **608**, respectively. Such a computation is denoted as $b_k = \mathbf{g}(b_i, b_j)$. Figure 6 also illustrates pseudo-random function R **518**, which is used to prepare table T_g **522**.

If one assumes initially that the fan-out of every gate is 1, table T_g contains four entries of the form:

$$c_i, c_j: (W_k^{g(b_i, b_j)}, c_k) \text{ XOR } R_{W_i^{b_i}}(c_j) \text{ XOR } R_{W_j^{b_j}}(c_i),$$

where $0 \leq i \leq j \leq 1$.

The value c_k is given by $c_k = \pi_k(b_k) = \pi_k(g(b_i, b_j))$. The entry does not have to include the index c_i, c_j since this is implicit in the entry's location.

Assume that ***A*** knows c_i, c_j and the values W_i^{bj}, W_j^{bj}. In order to compute a gate, ***A*** finds the entry c_i, c_j in the table T_g for that gate, and performs an XOR (exclusive-OR) operation with the value $R_{W_i^{bi}}(c_j)$ XOR $R_{W_j^{bj}}(c_i)$ to get the value $W_k^{bk} = W_k^{g(b_i, b_j)}$, and of c_k.

To code the Input the following is undertaken. Given the table T_g of the gates, and the garbled values W_i^{bi} and c_i which correspond to the input wires, it is easy to compute the garbled values of the output wires of the circuit. ***A*** knows the values of the input bits and should obtain the values of the corresponding wires. In step **528**, for each gate in circuit **506**, ***B*** sends to ***A*** the table T_g **522** that codes the gate. In step **530**, ***B*** sends to ***A*** the table T_O **526** that decrypts the garbled values of the output of the circuit the output bits of the circuit. In step **532**, for each gate input wire in the circuit, ***A*** and ***B*** engage in an Oblivious Transfer, at the end of which ***A*** learns the garbled value of the wire's input bit (but nothing about the garbled value of the input bit of the other wire into the gate), and ***B*** learns nothing.

A now has enough information to compute the circuit. In step **534**, ***A*** computes the output of the circuit for the input x. However, since ***A*** does not know the garbled values for any other input bits, ***A*** cannot compute information about $\boldsymbol{f}(x_0)$ for any $x_0 \neq x$ (except, of course, information that can be deduced from $\boldsymbol{f}(x)$ alone). Note that the communication between the two participants ***A*** and ***B*** can be done in a single back-and-forth round, and ***B*** can prepare the circuit in advance, before the input is known to ***A***.

To handle a gate fan-out greater than 1, it is simply required to use a different input to the pseudo-random function R at each gate in which the wire is used. (If the same value be used in different gates, then it will be possible to cancel the application of the pseudo-random function R by an XOR operation, and ***A*** could thereby learn relationships between garbled values.) Suppose that the fan-out of wire i is M, then in a gate m ($1 \leq m \leq M$) which uses wire i as input, the masking value that is used should be $R_{W_i^{bi}}(c_i, m)$. That is, the pseudo-random function R

should be applied to the concatenation of c_j and m. Alternatively, it is possible to assign each gate a unique identifier I_g, and use $R_{W_i^{b_i}}(c_j, I_g)$.

It is also possible to adapt this protocol to circuits in which gates have more than two inputs, as well as, for wires having more than two possible values. The size of the table for a gate with n inputs which each can have d values is d^n.

The prior art of REFERENCE 7 (Yao's protocol) is limited to two participants, but has been extended has been extended in the prior art to handle multi-party inputs, see REFERENCE 3.. These extended protocols, however, require a round of communication for each gate in the circuit, which is impractical in many applications, such as in auctions. The method of REFERENCE 3 would require extensive interactive communication among the bidders in an auction, and is therefore not suitable. In contrast, the present invention does not impose the burden of extensive interactive communication and does not require the bidders to communicate among themselves, and therefore represents an improvement not only over the prior art of REFERENCE 7 and 3. Furthermore, the prior art of REFERENCE 3 is secure only for limited coalitions of less than one-third of the parties.

A commitment to a value X is similar to the following process: party B which knows the value of X writes it on a piece of paper which is put in a sealed envelope. At this stage no one can learn anything about X, but B is committed to X and cannot change the value in the envelope. At a later stage B can "open the commitment" by opening the envelope and revealing X.

More formally, a commitment to a value X is computed by a function C=C(X,R), where R is a random string. It has the following properties: (1) C is easy to compute. (2) Given C(X,R), it is infeasible to compute any information about X. (3) There is an algorithm A such that A(C(X,R),X,R)=1, and for any other X' (different than X) and R' it holds with high probability that A(C(X,R),X',R')=0. Such commitments schemes can be implemented efficiently, see for example REFERENCE 5.

Now the details of the implementation of the preferred embodiment will be described in conjunction with the flow chart of Figure 4. The first stage is the announcement. This stage is carried out by the center **421** announcing in step **401** that it will compute F. Let K be a security parameter. The center constructs in step **402** K garbled circuits that compute F. For each input wire j of each of the circuits the center chooses in step **403** a random permutation P.sub.j over the two values 0 and 1. The center publishes in step **404** the tables of the gates of the K circuits **422**. For each input wire j (in each of the circuits) it publishes in step **404** a commitment to W.sub.j.sup.0 and a commitment to W.sub.j.sup.1, ordered by the permutation P.sub.j, and a commitment to P.sub.j.

The next stage is for the parties 420 to commit to their inputs. Each party B.sub.i has an input x.sub.i of l bits. The bits of this input are denoted as x.sub.(i,l). Each input bit should be input to an input wire in each of the K circuits. For each wire j of these wires, the center sends in step **405** to B.sub.i, the permutation P.sub.j. B.sub.i sends in response in step **406** a commitment **424** to P.sub.j(x.sub.(i,l)), i.e. to the permuted value of its input.

The next stage is to publish the commitments. The center **421** publishes in step **407** the commitments **424** it received from the parties.

The next stage is to open the commitments. The parties **420** choose K/2 of the K circuits that the center has created and ask the center to open in step **408** all the commitments to the permutations and garbled inputs of these K/2 circuits **423**. They verify in step **409** that these circuits indeed compute F. Each of the parties B.sub.i sends in step **410** its input x.sub.i to the center. B.sub.i also opens to the center the commitments that it made to each of its assigned input wires. These were for values 0 or 1 which are the permuted values of B.sub.i's inputs. The center verifies in step **411** that these commitments are consistent. The center publishes in step **412** the opened commitments **425** of each of the parties, and opens the garbled values W.sub.j.sup.0 or W.sub.j.sup.1 that correspond to them.

In the next stage, the center computes the function in step **413** and publishes the output of each of the K/2 circuits which were not chosen by the

parties.

In the final stage, each party **420** can verify the computations of the center **421.** Each B.sub.i can use the opened garbled values **425** and the tables of the gates **422** to compute the output of each of the K/2 circuits, and verify in step **414** that they all have the same output.

One problem that may be encountered in an auction is that a party does not open its commitment. For example, a party might refuse to communicate with the sender at the step at which the commitments should be open. This type of behavior enables cheating, for example, in the case of second price auctions the center itself might use fake identities of bidders in order to commit to bids in different values, and open only the bids which are smaller than the highest value among all other bids. This behavior might increase the amount that the winner would be required to pay.

One approach for dealing with parties that do not open their commitments appropriately would be to require parties to also submit their bids to a trusted third party T. The help of the trusted party T is not required, if all parties open their commitments. However, when a party refuses to open its commitment, the trusted party T can be called upon to open it. Such a scheme can be realized, for example, by using commitments of the following form: the public key of trusted partyT would be known to everyone. A commitment to a value v would be an encryption of this value with T's public key (say with a probabilistic encryption scheme which ensures indistinguishability). The party who created this commitment can open it by revealing v and showing how it encrypted it. If this party refuses to open the commitment then trusted party T can open it using its private key.

A more promising approach is to use "Timed commitments" [see REFERENCE 8]. These are commitment schemes with an optional forced opening phase enabling the receiver of the commitment to recover (with effort) the committed value without the help of the bidder making the commitment (committor). It is possible to require the bidders to use timed commitment schemes to commit to their bids, enabling the auctioneer to open these commitments, to their original value, if a bidder is not willing to open his or her bid.

A different approach for ensuring that each party opens its commitments is to require parties to back their commitments financially. A party who refuses to open its commitment would be required to pay a fine.

References

[1] M. Bellare and S. Micali, Non-interactive oblivious transfer and applications, Proc. Advances in Cryptology - Crypto '89, Springer-Verlag LNCS 435 (1990), 547-557.

[2] M. K. Franklin and M. K. Reiter, "The design and implementation of a secure auction server", IEEE Tran. on Software Engineering, 22(5), pp. 302-312, 1996.

[3] O. Goldreich, M. Micali, A. Wigderson, How to play any mental game, Proc. 19th ACM Symp. on Theory of Computing, 1987, pp. 218-229.

[4] M. Harakavy, J. D. Tygar and H. Kikuchi, "Electronic auctions with private bids", 3rd USENIX Workshop on Electronic Commerce, pp. 61-73, 1999.

[5] M. Naor, "Bit Commitment using Pseudo-randomness", J. of Cryptology, 4, 1991.

[6] M. Naor and B. Pinkas, "Privacy preserving negotiation and computation", patent application, 1999.

[7] A.C. Yao, How to Generate and Exchange Secrets, Proc. of the 27th IEEE Symp. on Foundations of Computer Science, 1986, pp. 162-167.

[8] D. Boneh and M. Naor, "Timed commitments and timed signatures", Proc. Advances in Cryptology - Crypto '00, Springer-Verlag LNCS, 2000.

Although the invention has been shown and described in terms of specific embodiments, nevertheless various changes and modifications will be evident to those skilled in the art from the teachings of the invention. Such changes and modifications which do not depart from the spirit, scope and contemplation of the invention are deemed to fall within the purview of the claims.

WHAT IS CLAIMED IS:

1. A method for preserving the integrity of a negotiation comprising the steps of:

a) providing an architecture which includes a center A, and a plurality of users B.sub.1, B.sub.2,..., B.sub.n,

b) generating for each user B.sub.i an input X.sub.i,

c) inputting each user's input X.sub.i to the center A,

d) computing and publishing a function F(X.sub.1,X.sub.2,...,X.sub.n) by the center A based on the input messages it receives,

e) each user B.sub.i (1<= i<= n) communicating with the center A exclusively, and

f) publishing by center A additional information which lets each of the users verify that F was computed correctly, and preventing a coalition of any one subset of the users from learning (i) anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, and (ii) information about the inputs of other users.

2. The method of Claim 1 for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount he has to pay.

3. The method according to any one of claims 1 or 2, for computing the output of a sealed bid auction, where the users are bidders and the center is the auctioneer, and wherein the input X.sub.i is the bid of bidder B.sub.i, and an output of F is the identity of the winning bidder and the amount to be paid, and wherein the center only makes disclosure to the winning bidder, while all other bidders being able to verify that the auction was computed correctly, but do not learn any other information.

4. The method according to any one of claims 1, 2 or 3, for first price auctions, where the output of F is (B.sub.j, X.sub.j), where X.sub.j is greater or equal to any one X.sub.i for 1 <=i <=n.

5. The method according to any one of claims 1, 2 or 3, for second price auctions (Vickrey auctions), where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is greater or equal to any X.sub.i for 1 <=i <=n except for i=j1.

6. The method according to any one of claims 1, 2 or 3, for k-th price auctions, where the output of F is (B.sub.j1, X.sub.j2), where X.sub.j1 is greater or equal to any X.sub.i for 1 <=i <=n, and X.sub.j2 is the k-th largest among all inputs X.sub.i for 1 <=i <=n.

7. The method according to any one of the preceding claims wherein the auction is a plural auction where there are a plurality of sellers.

8. The method according to any one of the preceding claims wherein the auction is a generalized Vickrey auction.

9. The method according to any one of the preceding claims, comprising the step of, computing the auction such that the auctioneer wants to buy an item and each of the bidders wants to sell this item, and wherein negative values of the inputs X.sub.i are possible.

10. The method according to any one of the preceding claims, comprising the step of; computing the output of the auction such that the users learn, in addition, some statistic of the inputs, such as, the users can learn at least one of the average of the inputs, the variance of the inputs, or how many one inputs were in a certain range.

11. The method according to any one of the preceding claims, comprising the step of computing the output of the function such that only the center learns the output of the function. or several of the users learn the output of the function, or all the users learn the output of the function.

12. The method according to any one of the preceding claims, comprising the step of, computing the output of a mechanism, in particular, for one of Groves-Clark mechanisms, opinion polling and stable matching.

13. The method according to any one of the preceding claims, comprising the steps of each user committing to the values of his input in a manner that the user cannot change it afterwards, but hiding the input value from the center,.at a specific stage, the users opening their commitments to their inputs and revealing their values to the center, which then computes the value of F in a manner the each of the users can verify that the values that were used as inputs for computing F were the values that were committed to by the users.

14. The method according to any one of the preceding claims, comprising the step of implementing automated agents which participate in the auction which do not disclose to the auctioneer the limit price that they were given, until the end of the bidding period.

15. The method according to any one of the preceding claims, comprising the step of computing a function where the center can generate a proof that it computed the correct output of the function.

16. The method according to any one of the preceding claims, comprising the step of computing a function by N centers, such that only if K of the N centers collude they can learn information about the parties' inputs.

17. In a system that contains N parties, each having a private input, and a center adapted to compute a function F of said input; apparatus for computing said function F in said center, comprising:

a first program provided in the center that enables calculation of said function F;

circuitry for publishing said function F using the program while not revealing substantially any information about said input; and

a second program provided to the parties enabling each one of said parties to prove that said function F was calculated correctly.

18. In a system according to claim 17, wherein the second program precludes the learning of any information other than the function F was calculated correctly.

19. In a system according to claim 17, wherein the first program includes a construction of K garbled circuits for computing function F.

20. In a system according to claim 17, wherein said parties are bidders in an auction; said input are bids, said center is an auctioneer, said function F is the rule by which said auction is decided, whereby the auctioneer is capable of calculating the result of said auction without revealing any information about said bids, except for the identity of the winning party from among said parties, and the amount to pay.

21. In a system according to claim 20, wherein the function is determined utilizing a circuit of gates.

22. In a system according to claim 20, wherein the second program includes the capability of utilizing the circuit of gates to independently determine and verify that the computations of the center are correct.

Page 5 of 9 Doc 7 of 9

ABSTRACT

A method and system for preserving the integrity of a negotiation that includes providing an architecture which includes a center A, and a plurality of users B.sub.1, B.sub.2,..., B.sub.n. each user B.sub.i generates an input X.sub.i, which is input to the center A. The center A computes and publishes a function F(X.sub.1,X.sub.2,...,X.sub.n) based on the input messages it receives. Each user B.sub.i (1<= i<= n) communicates with the center A, exclusively. Center A publishes additional information which lets each of the users verify that F was computed correctly, and prevents a coalition of any one subset of the users from learning anything which cannot be computed just from the output of the function, F(X.sub.1,...,X.sub.n), and from their own inputs, or information about the inputs of other users.

T0804P60260

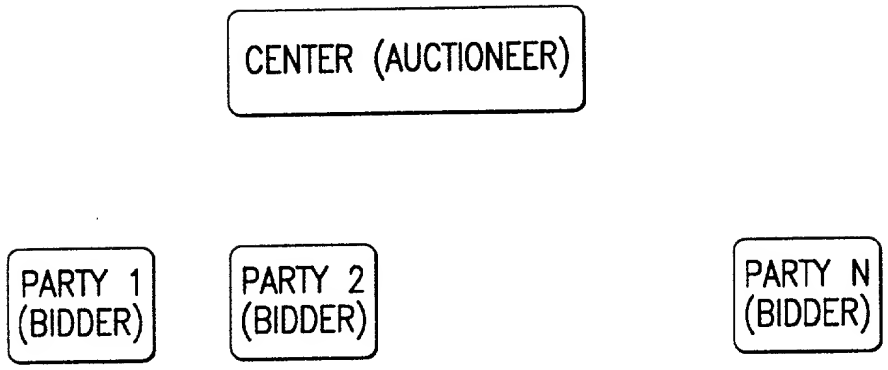


FIG.1

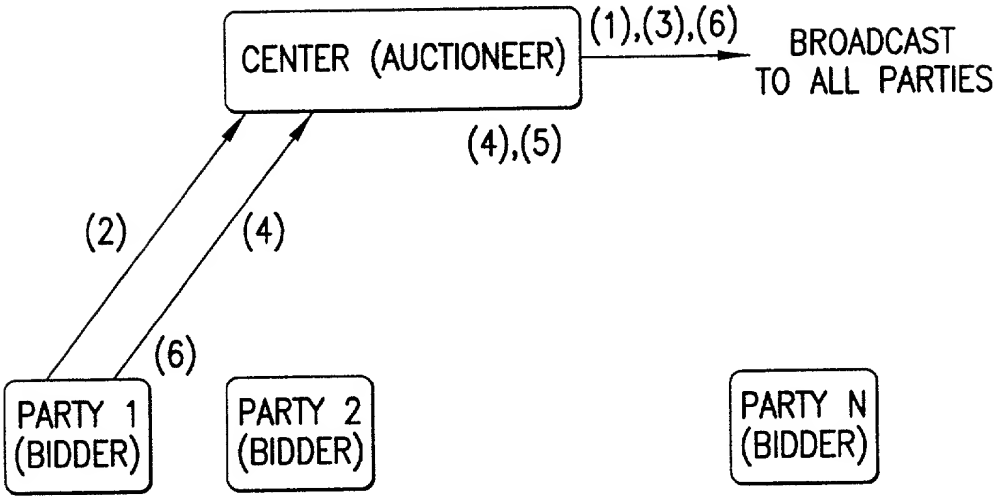


FIG.2

T0804D "09807099

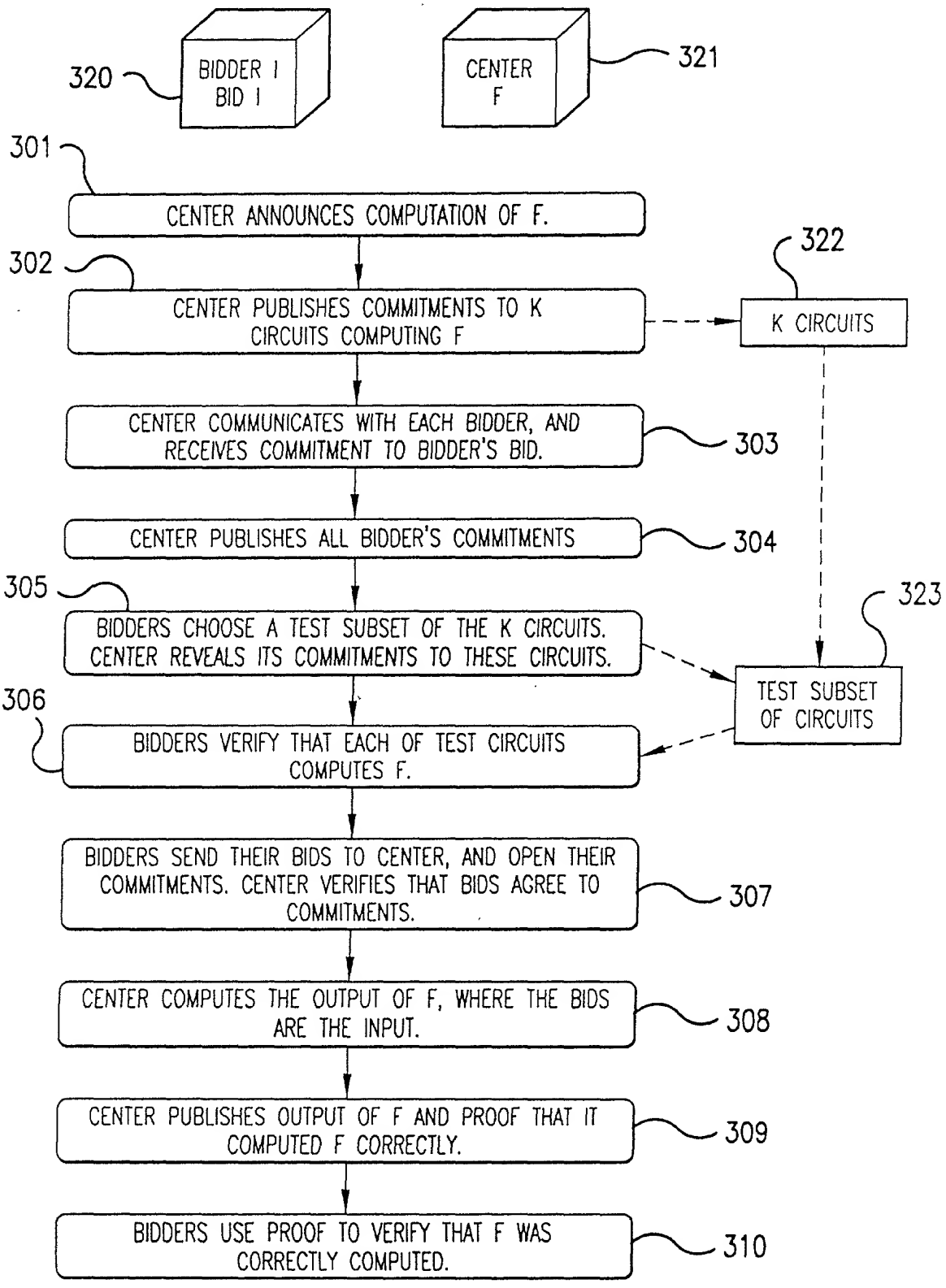

320
BIDDER I
BID I
CENTER
F
321
301
CENTER ANNOUNCES COMPUTATION OF F.
302
CENTER PUBLISHES COMMITMENTS TO K CIRCUITS COMPUTING F
322
K CIRCUITS
CENTER COMMUNICATES WITH EACH BIDDER, AND RECEIVES COMMITMENT TO BIDDER'S BID.
303
CENTER PUBLISHES ALL BIDDER'S COMMITMENTS
304
305
BIDDERS CHOOSE A TEST SUBSET OF THE K CIRCUITS. CENTER REVEALS ITS COMMITMENTS TO THESE CIRCUITS.
323
TEST SUBSET OF CIRCUITS
306
BIDDERS VERIFY THAT EACH OF TEST CIRCUITS COMPUTES F.
BIDDERS SEND THEIR BIDS TO CENTER, AND OPEN THEIR COMMITMENTS. CENTER VERIFIES THAT BIDS AGREE TO COMMITMENTS.
307
CENTER COMPUTES THE OUTPUT OF F, WHERE THE BIDS ARE THE INPUT.
308
CENTER PUBLISHES OUTPUT OF F AND PROOF THAT IT COMPUTED F CORRECTLY.
309
BIDDERS USE PROOF TO VERIFY THAT F WAS CORRECTLY COMPUTED.
310

FIG.3

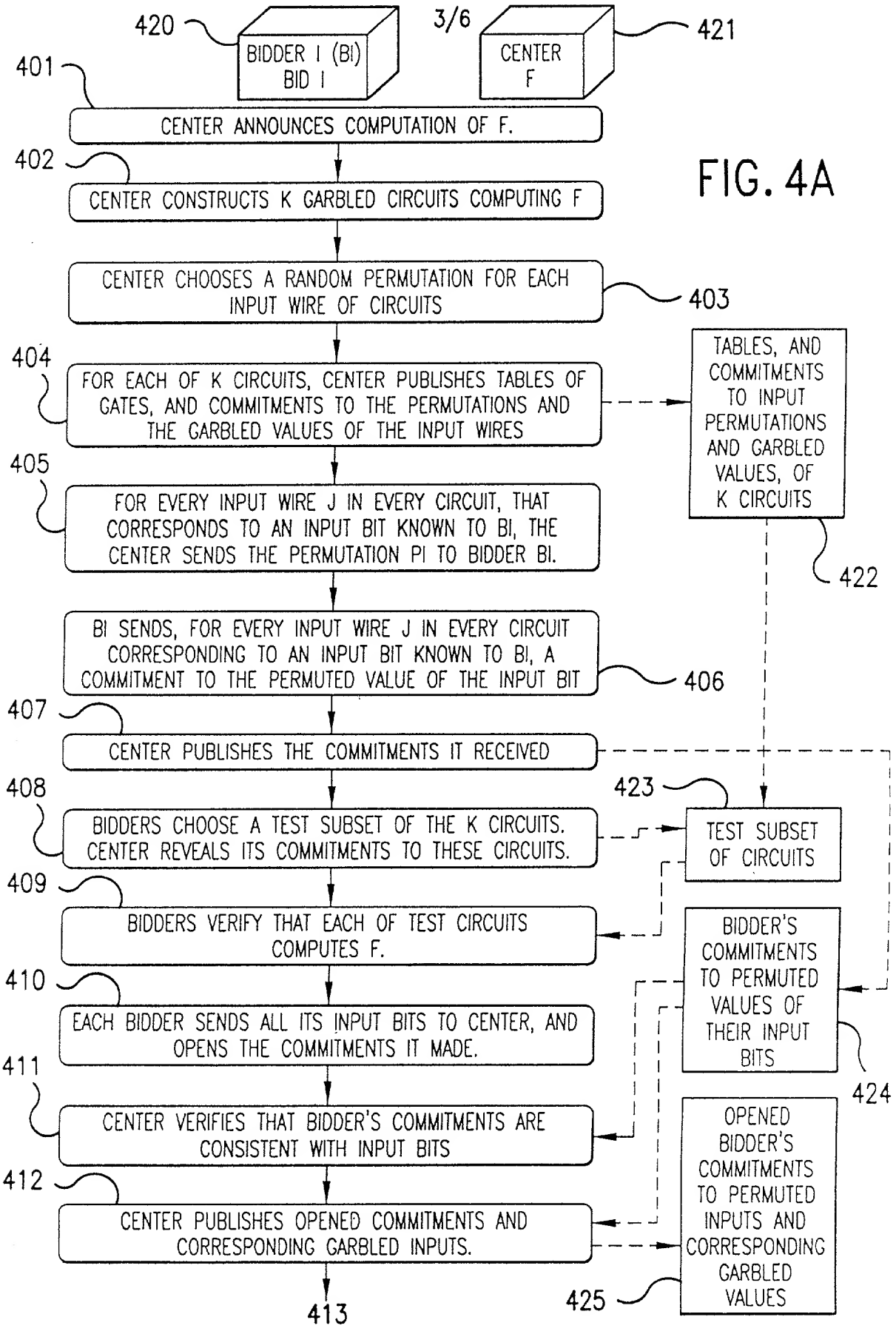


FIG. 4A

"D6040"650/0860

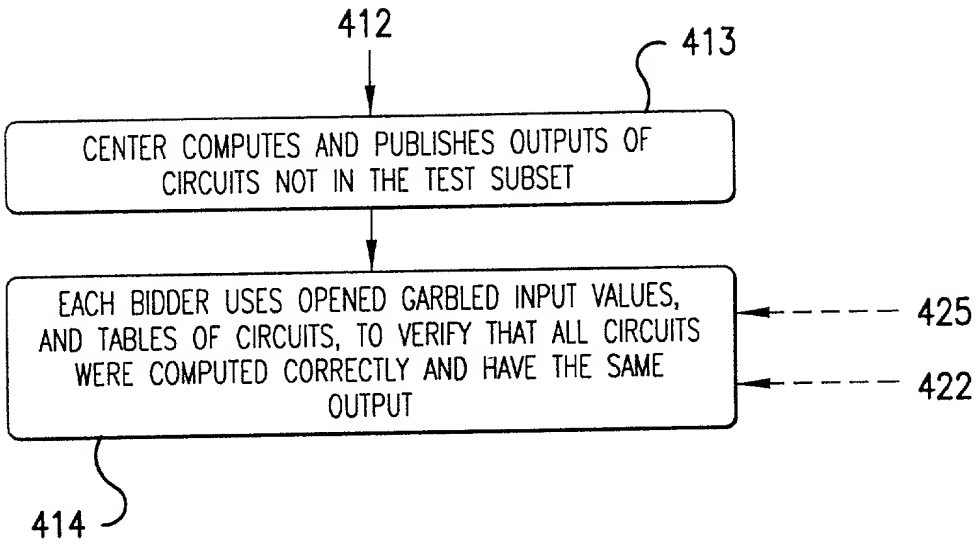


FIG. 4B

EL606470650US

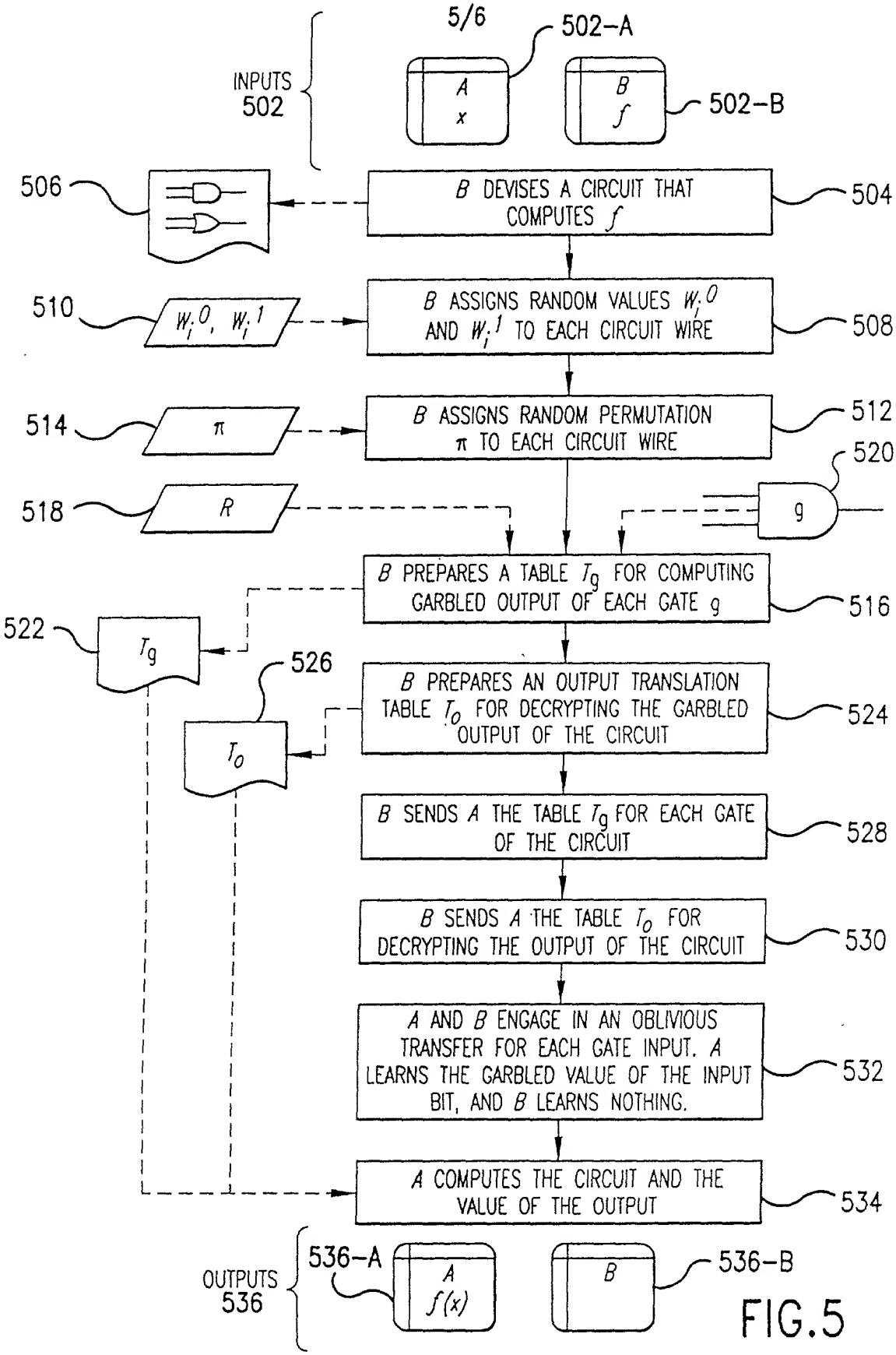


FIG.5

Express Mail Label No. EV080470860

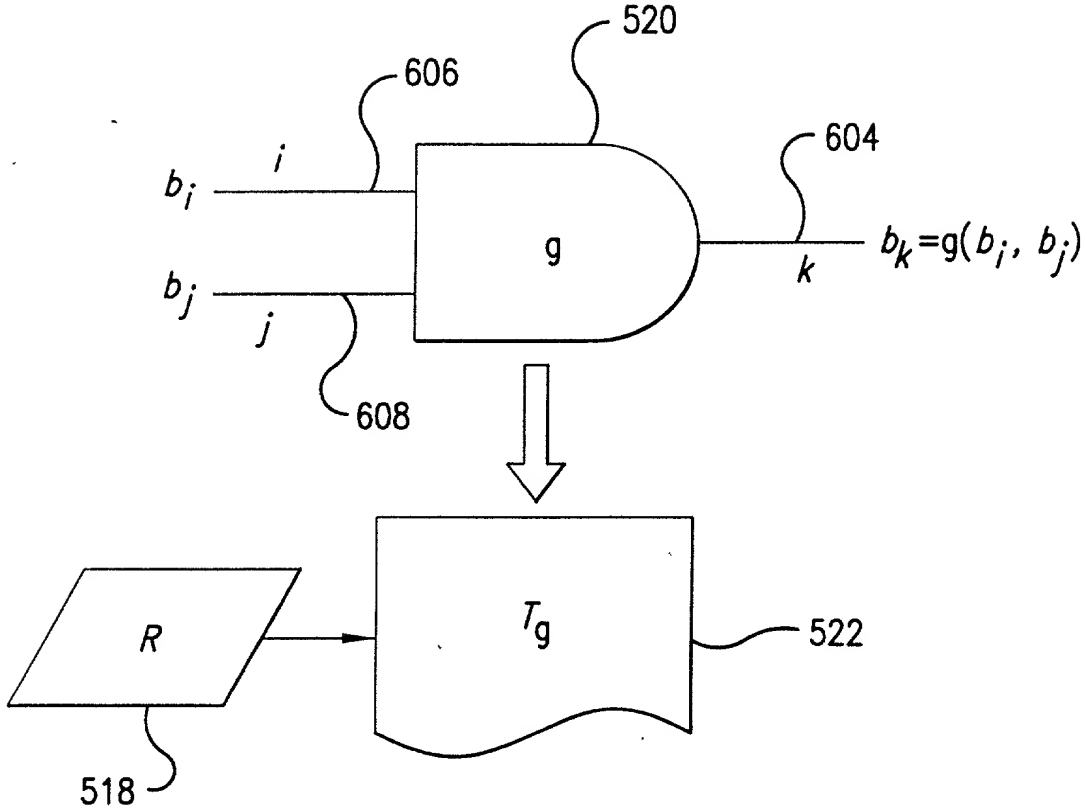


FIG.6

EL604170" 6504208 US

PCT/US00/21615

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

HONESTY PRESERVING NEGOTIATION AND COMPUTATION

the specification of which: (check one)

____ is attached hereto.

__X__ was filed on August 8, 2000
under Attorney's Docket Number 704-X00-047PCT
as PCT International Application Serial No. PCT/US 00/21615
and was amended on (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 CFR 1.56.

I hereby claim the benefit of foreign priority under 35 USC 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate or of any PCT international application having a filing date before that of the application the priority of which is claimed:

Prior Foreign Application(s):			Priority Claimed	
Number	Country	Filing Date	Yes	No
60/148,183	US	08/10/99	X	

I hereby claim the benefit under 35 USC 119(e) of any United States provisional application(s) listed below

Application Number	Filing Date
60/148,183	08/10/99

I hereby claim the benefit of United States priority under 35 USC 120 of any United States application(s) or 365(c) of any PCT international applications designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in a listed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

U.S. Parent Application or PCT Parent Number	(Filing Date)	Parent Patent Number
PCT/US 00/21615	AUG. 8, 2000	

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

3

Martin Fleit Reg. No. 16,900
Robert C. Kain Reg. No. 30,648
Jon A. Gibbons Reg. No. 37,333
Stephen C. Bongini Reg. No. 40,917
Jose Gutman Reg. No. 35,171

Send correspondence to MARTIN FLEIT, Fleit, Kain, Gibbons, Gutman & Bongini, P.L., 520 Brickell Key Drive, Miami, Florida 33131, and direct all telephone calls to MARTIN FLEIT at (305) 536-9020.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FOSSATO-SOSNOFF-GOLDSTEIN

1-DD

FULL NAME OF INVENTOR: BINYAMIN PINKAS

INVENTOR'S SIGNATURE: _____ DATE: April 5, 2001

RESIDENCE: JERSEY CITY, NEW JERSEY, USA NJ.
CITIZENSHIP: ISRAELI
POST OFFICE ADDRESS: 1 RIVER COURT, JERSEY CITY, NJ 07310

FULL NAME OF INVENTOR: SIMEON NAOR

INVENTOR'S SIGNATURE: _____ DATE:
RESIDENCE: TEL AVIV, ISRAEL
CITIZENSHIP: ISRAELI
POST OFFICE ADDRESS: 5 BET ZURI STREET, APT 5, TEL AVIV 69122, ISRAEL

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name;

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

HONESTY PRESERVING NEGOTIATION AND COMPUTATION

the specification of which: (check one)

____ is attached hereto.

__X__ was filed on August 8, 2000
under Attorney's Docket Number 704-X00-047PCT
as PCT International Application Serial No. PCT/US 00/21615
and was amended on (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the patentability of this application in accordance with 37 CFR 1.56.

I hereby claim the benefit of foreign priority under 35 USC 119(a)-(d) or 365(b) of any foreign application(s) for patent or inventor's certificate, or 365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate or of any PCT international application having a filing date before that of the application the priority of which is claimed:

Prior Foreign Application(s):			Priority Claimed	
Number	Country	Filing Date	Yes	No
60/148,183	US	08/10/99	X	

I hereby claim the benefit under 35 USC 119(e) of any United States provisional application(s) listed below

Application Number	Filing Date
60/148,183	08/10/99

05 Apr 01 22:51 p.2

I hereby claim the benefit of United States priority under 35 USC 120 of any United States application(s) or 365(c) of any PCT international applications designating the United States of America, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in a listed in the prior United States or PCT international application in the manner provided by the first paragraph of 35 USC 112, I acknowledge the duty to disclose information material to the patentability of this application as defined in 37 CFR 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

U.S. Parent Application or PCT Parent Number	(Filing Date)	Parent Patent Number
PCT/US 00/21615	AUG. 8, 2000	

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.

Martin Fleit	Reg. No. 16,900
Robert C. Kain	Reg. No. 30,648
Jon A. Gibbons	Reg. No. 37,333
Stephen C. Bongini	Reg. No. 40,917
Jose Gutman	Reg. No. 35,171

Send correspondence to MARTIN FLEIT, Fleit, Kain, Gibbons, Gutman & Bongini, P.L., 520 Brickell Key Drive, Miami, Florida 33131, and direct all telephone calls to MARTIN FLEIT at (305) 536-9020.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 USC 1001 and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

FULL NAME OF INVENTOR: BINYAMIN PINKAS

INVENTOR'S SIGNATURE: _____ DATE:

RESIDENCE: JERSEY CITY, NEW JERSEY, USA
CITIZENSHIP: ISRAELI
POST OFFICE ADDRESS: 1 RIVER COURT, JERSEY CITY, NJ 07310

2-00

FULL NAME OF INVENTOR: SIMEON NAOR

INVENTOR'S SIGNATURE: _____ DATE: April 5th 2001
RESIDENCE: TEL AVIV, ISRAEL
CITIZENSHIP: ISRAELI ILX
POST OFFICE ADDRESS: 5 BET ZURI STREET, APT 5, TEL AVIV 69122, ISRAEL

P.03 05 Apr 01 22:51